Practitioner's Docket No. U 013188-5 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Number:	US 7,100,051 B1
Issued:	August 29, 2006
Name of Patentee:	Avid KIPNIS, et al
Title of Invention:	PUBLIC-KEY SIGNATURE METHODS AND SYSTEMS

Certificate of Correction Branch
Director of the United States Patent and Trademark Office
P. O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Certificate of Correction Branch
of the Office of Patent Publication

REQUEST FOR CERTIFICATE OF CORRECTION OF PATENT FOR PTO MISTAKE (37 C.F.R. §1.322(a))

NOTE: "If such a request for correction was incurred through the fault of the United States Patent and Trademark Office (Office), and is clearly disclosed in the records of the Office, and is accompanied by documentation that unequivocally supports the patentee's assertion(s), a Certificate of Correction will be expeditiously issued. Such supporting documentation can consist of relevant photocopied receipts, manuscript pages, correspondence dated and received by the Office, photocopies of Examiners' responses regarding entry of amendments, or any other validation that supports the patentee's request so that the request can be processed without the patent file." Notice of September 17, 2002, 1262 OG 96.

1. Attached is Form PTO—1050 (PTO/SB/44) suitable for printing.

NOTE: Form PTO-1050 (or PTO/SB/44), using the column and line number in the printed patent, should be used exclusively regardless of the length or complexity of the subject matter. M.P.E.P. § 1485, 7th ed.

NOTE: The patent grant should be retained by the patentee. The PTO does not attach the Certificate of Correction to the patentee's copy of the patent. The patent grant will be returned to the patentee if submitted. M.P.E.P. § 1485, 8th ed.

2. The exact page and line number where the errors are shown correctly in the application file are:

NOTE: The exact page and line number where the errors occur in the application file should be identified on the request. However, on form PTO/SB/44, only the column and line number in the printed patent should be used. M.P.E.P. § 1480, 8th Edition.

Amendment of November 23, 2005 (copy of pages 2-10 attached-- see claims 1 and 35).

Date: September 11, 2008

3. **Please send the Certificate to:**

Name: CLIFFORD J. MASS

Address: c/o Ladas & Parry LLP
26 West 61st Street
New York, NY 10023

(complete, if applicable)

Signature(s) of patentee(s)

or

Signature of assignee or person authorized to sign on behalf of assignee

NDS LIMITED

(type or print name of assignee)

☒ Assignment recorded on

February 5, 2001

Reel 011507
Frame 0255

CP8 TECHNOLOGIES

(type or print name of assignee)

☒ Assignment recorded on

May 10, 2006

Reel 017608
Frame 0290

Clifford J. Mass 25858 (212) 708-1890
(type or print name of authorized person signing)

attorney of record who acts on behalf of assignee

☐ Recordal of assignment attached

☐ Attached is a "STATEMENT UNDER 37 CFR 3.73(b)," establishing the right of the assignee to take action in this case.

NOTE: "A certificate of correction, under 35 U.S.C. 254, may be issued at the request of the patentee or [the patentee's] assignee." 37 C.F.R. § 1.322(a). The certificate of correction can be signed by the attorney of record who acts on behalf of the inventor(s) or assignee(s).

PTO/SB/44 (02-01)
Approved for use through 1/31/2004. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO.: US 7,100,051B1
DATED : August 29, 2006
INVENTOR(S): Aviad KIPNIS, et al

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In claim 1, col. 35, line 22, "functions $P_k''(a_1,...$" should read --functions $P_l''(a_1,...,$--

In claim 36, col. 40, line 15, "a_{n+v}" should read --a_{n+v},--

MAILING ADDRESS OF SENDER:
Clifford J. Mass
c/o Ladas & Parry LLP
26 West 61st Street
New York, N.Y. 10023
Reg. No. 30086
Tel. No. (212) 708-1890

PATENT NO. US7,100,051 B1

No. of additional copies

IN THE CLAIMS

Claim 1 (currently amended) A digital signature cryptographic method, performed by a computing device, the method comprising:

supplying a set S1 of k polynomial functions as a public-key, the set S1 including the functions $P_1(x_1,...,x_{n+v}, y_1,...,y_k),..., P_k(x_1,...,x_{n+v}, y_1,...,y_k)$, where k, v, and n are integers, $x_1,...,x_{n+v}$ are n+v variables of a first type, $y_1,...,y_k$ are k variables of a second type, and the set S1 is obtained by applying a secret key operation on a set S2 of k polynomial functions $P'_1(a_1,...,a_{n+v},y_1,...,y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$ where $a_1,...,a_{n+v}$ are n+v variables which include a set of n "oil" variables $a_1,...,a_n$, and a set of v "vinegar" variables $a_{n+1},...,a_{n+v}$, the supplying comprising selecting the number v of "vinegar" variables to be greater than the number n of "oil" variables;

providing a message to be signed;

applying a hash function on the message to produce a series of k values $b_1,...,b_k$;

substituting the series of k values $b_1,...,b_k$ for the variables $y_1,...,y_k$ of the set S2 respectively to produce a set S3 of k polynomial functions $P''_1(a_1,...,a_{n+v}),...,P''_k(a_1,...,a_{n+v})$;

selecting v values $a'_{n+1},...,a'_{n+v}$ for the v "vinegar" variables $a_{n+1},...,a_{n+v}$;

solving a set of equations $P''_1(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0,...,P''_k(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0$ to obtain a solution for $a'_1,...,a'_n$; ~~and~~

applying the secret key operation to transform $a'_1,...,a'_{n+v}$ to a digital signature $e_1,...,e_{n+v}$; and

assigning $e_1,...,e_{n+v}$ as the digital signature of the message.

Claim 2 (previously presented) A method according to claim 1 and also comprising verifying the digital signature.

Claim 3 (previously presented) A method according to claim 2 and wherein said verifying comprises:

obtaining the signature $e_1,...,e_{n+v}$, the message, the hash function and the public key;

applying the hash function on the message to produce the series of k values $b_1,\ldots,b_k$; and

verifying that the equations $P_1(e_1,\ldots,e_{n+v},b_1,\ldots,b_k)=0,\ldots, P_k(e_1,\ldots,e_{n+v}, b_1,\ldots,b_k)=0$ are satisfied.

Claim 4 (previously presented) A method according to claim 1 and wherein the method comprises an HFEV scheme and the set S2 comprises a set f(a) of k polynomial functions of the HFEV scheme.

Claim 5 (previously presented) A method according to claim 1 and wherein the method comprises a UOV scheme and the set S2 comprises a set S of k polynomial functions of the UOV scheme.

Claim 6 (canceled)

Claim 7 (previously presented) A method according to claim 1 and wherein v is selected such that q^v is greater than 2^{32}, where q is the number of elements of a finite field K over which the sets S1, S2 and S3 are provided.

Claim 8 (previously presented) A method according to claim 1 and wherein said supplying comprises obtaining the set S1 from a subset S2' of k polynomial functions of the set S2, the subset S2' being characterized in that all coefficients of components involving any of the $y_1,\ldots,y_k$ variables in the k polynomial functions $P'_1(a_1,\ldots,a_{n+v},y_1,\ldots,y_k),\ldots,P'_k(a_1,\ldots,a_{n+v},y_1,\ldots,y_k)$ are zero, and the number v of "vinegar" variables is greater than the number n of "oil" variables.

Claim 9 (previously presented) A method according to claim 8 and wherein the set S2 comprises a set S of k polynomial functions of a UOV scheme, and the number v of "vinegar" variables is selected to satisfy one of the following conditions:

(a) for each characteristic p other than 2 of a field K in an "Oil and Vinegar" scheme of degree 2, v satisfies the inequality $q^{(v-n)-1} * n^4 > 2^{40}$, where K is a finite field over which the sets S1, S2 and S3 are provided,

(b) for p = 2 in an "Oil and Vinegar" scheme of degree 3, v is greater than $n*(1 + \text{sqrt}(3))$ and less than or equal to $n^3/6$, and

(c) for each p other than 2 in an "Oil and Vinegar" scheme of degree 3, v is greater than n and less than or equal to n^4.

Claim 10 (previously presented) A method according to claim 8 and wherein the set S2 comprises a set S of k polynomial functions of a UOV scheme, and the number v of "vinegar" variables is selected to satisfy the inequalities $v<n^2$ and $q^{(v-n)-1} * n^4 > 2^{40}$ for a characteristic p=2 of a field K in an "Oil and Vinegar" scheme of degree 2, where K is a finite field over which the sets S1, S2 and S3 are provided and q is the number of elements of K.

Claim 11 (original) A method according to claim 1 and wherein said secret key operation comprises a secret affine transformation s on the n+v variables $a_1,...,a_{n+v}$.

Claim 12 (original) A method according to claim 4 and wherein said set S2 comprises an expression including k functions that are derived from a univariate polynomial.

Claim 13 (original) A method according to claim 12 and wherein said univariate polynomial includes a univariate polynomial of degree less than or equal to 100,000.

Claim 14 (original) A cryptographic method for verifying the digital signature of claim 1, the method comprising:

obtaining the signature $e_1,...,e_{n+v}$, the message, the hash function and the public key;

applying the hash function on the message to produce the series of k values $b_1,\ldots,b_k$; and

verifying that the equations $P_1(e_1,...,e_{n+v},b_1,\ldots,b_k)=0,\ldots, P_k(e_1,...,e_{n+v}, b_1,\ldots,b_k)=0$ are satisfied.

Claims 15 – 17 (canceled)

Claim 18 (currently amended) A computer system for generating a signature, ~~generator~~ comprising:

a signature input receiver operative to receive a set S1 of k polynomial functions as a public-key and a message to be signed, the set S1 including the functions $P_1(x_1,...,x_{n+v}, y_1,...,y_k),..., P_k(x_1,...,x_{n+v}, y_1,...,y_k)$, where k, v, and n are integers, $x_1,...,x_{n+v}$ are n+v variables of a first type, $y_1,...,y_k$ are k variables of a second type, and the set S1 is obtained by applying a secret key operation on a set S2 of k polynomial functions $P'_1(a_1,...,a_{n+v},y_1,...,y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$, where $a_1,...,a_{n+v}$ are n+v variables which include a set of n "oil" variables $a_1,...,a_n$, and a set of v "vinegar" variables $a_{n+1},...,a_{n+v}$ and the number v of "vinegar" variables is greater than the number n of "oil" variables; and

a signature processor operatively associated with the signature input receiver and operative to perform the following operations:

to apply a hash function on the message to produce a series of k values $b_1,...,b_k$,

to substitute the series of k values $b_1,...,b_k$ for the variables $y_1,...,y_k$ of the set S2 respectively to produce a set S3 of k polynomial functions $P''_1(a_1,...,a_{n+v}),..., P''_k(a_1,...,a_{n+v})$,

to select v values $a'_{n+1},...,a'_{n+v}$ for the v "vinegar" variables $a_{n+1},...,a_{n+v}$;

to solve a set of equations $P''_1(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0,...,$ $P''_k(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0$ to obtain a solution for $a'_1,...,a'_n$; ~~and~~

to apply the secret key operation to transform $a'_1,...,a'_{n+v}$ into a digital signature $e_1,...,e_{n+v}$; and

to assign $e_1,....,e_{n+v}$ as the digital signature of the message.

Claim 19 (previously presented) Apparatus according to claim 18 and also comprising a signature verifier operatively associated with the signature processor and operative to verify the digital signature.

Claim 20 (previously presented) Apparatus according to claim 19 and wherein said signature verifier is operative to verify the digital signature by performing the following operations:

obtaining the signature $e_1,...,e_{n+v}$, the message, the hash function and the public key;

applying the hash function on the message to produce the series of k values $b_1,\ldots,b_k$; and

verifying that the equations $P_1(e_1,...,e_{n+v},b_1,\ldots,b_k)=0,\ldots, P_k(e_1,...,e_{n+v}, b_1,\ldots,b_k)=0$ are satisfied.

Claim 21 (previously presented) Apparatus according to claim 18 and wherein the signature processor is operative to perform an HFEV scheme, and the set S2 comprises a set f(a) of k polynomial functions of the HFEV scheme.

Claim 22 (previously presented) Apparatus according to claim 18 and wherein the signature processor is operative to perform a UOV scheme, and the set S2 comprises a set S of k polynomial functions of the UOV scheme.

Claim 23 (canceled)

Claim 24 (previously presented) Apparatus according to claim 18 and wherein v is selected such that q^v is greater than 2^{32}, where q is the number of elements of a finite field K over which the sets S1, S2 and S3 are provided.

Claim 25 (previously presented) Apparatus according to claim 18 and wherein the set S1 is obtained from a subset S2' of k polynomial functions of the set S2, the subset S2' being characterized in that all coefficients of components involving any of the $y_1,\ldots,y_k$ variables in the k polynomial functions $P'_1(a_1,...,a_{n+v},y_1,\ldots,y_k)$, $\ldots,P'_k(a_1,...,a_{n+v},y_1,\ldots,y_k)$ are zero, and the number v of "vinegar" variables is greater than the number n of "oil" variables.

Claim 26 (previously presented) Apparatus according to claim 25 and wherein the set S2 comprises a set S of k polynomial functions of a UOV scheme, and the number v of "vinegar" variables is selected to satisfy one of the following conditions:

(a) for each characteristic p other than 2 of a field K in an "Oil and Vinegar" scheme of degree 2, v satisfies the inequality $q^{(v-n)-1} * n^4 > 2^{40}$, where K is a finite field over which the sets S1, S2 and S3 are provided,

(b) for p = 2 in an "Oil and Vinegar" scheme of degree 3, v is greater than n*(1 + sqrt(3)) and less than or equal to $n^3/6$, and

(c) for each p other than 2 in an "Oil and Vinegar" scheme of degree 3, v is greater than n and less than or equal to n^4.

Claim 27 (previously presented) Apparatus according to claim 25 and wherein the set S2 comprises a set S of k polynomial functions of a UOV scheme, and the number v of "vinegar" variables is selected to satisfy the inequalities $v<n^2$ and $q^{(v-n)-1} * n^4 > 2^{40}$ for a characteristic p=2 of a field K in an "Oil and Vinegar" scheme of degree 2, where K is a finite field over which the sets S1, S2 and S3 are provided and q is the number of elements of K.

Claim 28 (previously presented) Apparatus according to claim 18 and wherein said secret key operation comprises a secret affine transformation s on the n+v variables $a_1,...,a_{n+v}$.

Claim 29 (previously presented) Apparatus according to claim 21 and wherein said set S2 comprises an expression including k functions that are derived from a univariate polynomial.

Claim 30 (previously presented) Apparatus according to claim 29 and wherein said univariate polynomial includes a univariate polynomial of degree less than or equal to 100,000.

Claim 31 (previously presented) A signature verifier for verifying the digital signature generated by the signature generator of claim 18, the signature verifier comprising a verifier processor operative to perform the following operations:

to obtain the signature $e_1,...,e_{n+v}$, the message, the hash function and the public key via the signature input receiver;

to apply the hash function on the message to produce the series of k values $b_1,\ldots,b_k$; and

to verify that the equations $P_1(e_1,...,e_{n+v},b_1,\ldots,b_k)=0,\ldots, P_k(e_1,...,e_{n+v}, b_1,\ldots,b_k)=0$ are satisfied.

Claims 32 – 34 (canceled)

Claim 35 (currently amended) A digital signature <u>generated by a computer system, the digital signature</u> comprising:

a signature $e_1,...,e_{n+v}$ generated by processing a set S1 of k polynomial functions provided as a public-key and a message to be signed, where the set S1 includes functions $P_1(x_1,...,x_{n+v}, y_1,\ldots,y_k),\ldots, P_k(x_1,...,x_{n+v}, y_1,\ldots,y_k)$, where k, v, and n are integers, $x_1,...,x_{n+v}$ are n+v variables of a first type, $y_1,\ldots,y_k$ are k variables of a second type, and the set S1 is obtained by applying a secret key operation on a set S2 of k polynomial functions $P'_1(a_1,...,a_{n+v},y_1,\ldots,y_k),\ldots,P'_k(a_1,...,a_{n+v},y_1,\ldots,y_k)$ where $a_1,...,a_{n+v}$ are n+v variables which include a set of n "oil" variables $a_1,...,a_n$, and a set of v "vinegar" variables $a_{n+1},...,a_{n+v}$, and the number v of "vinegar" variables is greater than the number n of "oil" variables, so that a hash function applied on the message to produce a series of k values $b_1,\ldots,b_k$ that are substituted for the variables $y_1,\ldots,y_k$ of the set S2 respectively to produce a set S3 of k polynomial functions $P''_1(a_1,...,a_{n+v}),\ldots, P''_k(a_1,...,a_{n+v})$ and v values $a'_{n+1},...,a'_{n+v}$ that are selected for the v "vinegar" variables $a_{n+1},...,a_{n+v}$, enable to solve a set of equations $P''_1(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0,\ldots, P''_k(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0$ to obtain a solution for $a'_1,...,a'_n$, and application of the secret key operation transforms $a'_1,...,a'_{n+v}$ into ~~the digital signature~~ $e_1,...,e_{n+v}$ <u>which is assigned as the digital signature of the message</u>.

Claim 36 (previously presented) A digital signature produced by the method of claim 1.

Claim 37 (previously presented) A method according to claim 1 and wherein said supplying comprises obtaining the set S1 from a subset S2' of k polynomial functions of the set S2, the subset S2' being characterized in that all coefficients of components involving orders higher than 1 of any of the n "oil" variables $a_1,\ldots,a_n$ and coefficients of components involving multiplication of two or more of the n "oil" variables $a_1,\ldots,a_n$ in the k polynomial functions $P'_1(a_1,\ldots,a_{n+v},y_1,\ldots,y_k)$, $\ldots,P'_k(a_1,\ldots,a_{n+v},y_1,\ldots,y_k)$ are zero, and the number v of "vinegar" variables is greater than the number n of "oil" variables.

Claim 38 (previously presented) A method according to claim 37 and wherein the set S2 comprises a set S of k polynomial functions of a UOV scheme, and the number v of "vinegar" variables is selected to satisfy one of the following conditions:

(a) for each characteristic p other than 2 of a field K in an "Oil and Vinegar" scheme of degree 2, v satisfies the inequality $q^{(v-n)-1} * n^4 > 2^{40}$, where K is a finite field over which the sets S1, S2 and S3 are provided,

(b) for p = 2 in an "Oil and Vinegar" scheme of degree 3, v is greater than n*(1 + sqrt(3)) and less than or equal to $n^3/6$, and

(c) for each p other than 2 in an "Oil and Vinegar" scheme of degree 3, v is greater than n and less than or equal to n^4.

Claim 39 (previously presented) A method according to claim 37 and wherein the set S2 comprises a set S of k polynomial functions of a UOV scheme, and the number v of "vinegar" variables is selected to satisfy the inequalities $v<n^2$ and $q^{(v-n)-1} * n^4 > 2^{40}$ for a characteristic p=2 of a field K in an "Oil and Vinegar" scheme of degree 2, where K is a finite field over which the sets S1, S2 and S3 are provided and q is the number of elements of K.

Claim 40 (previously presented) Apparatus according to claim 18 and wherein the set S1 is obtained from a subset S2' of k polynomial functions of the set S2, the subset S2' being characterized in that all coefficients of components involving orders higher than 1 of any of the n "oil" variables $a_1,\ldots,a_n$ and coefficients of components involving multiplication of two or more of the n "oil" variables $a_1,\ldots,a_n$ in the k polynomial

functions $P'_1(a_1,...,a_{n+v},y_1,...,y_k)$, ...,$P'_k(a_1,...,a_{n+v},y_1,...,y_k)$ are zero, and the number v of "vinegar" variables is greater than the number n of "oil" variables.

Claim 41 (previously presented) Apparatus according to claim 40 and wherein the set S2 comprises a set S of k polynomial functions of a UOV scheme, and the number v of "vinegar" variables is selected to satisfy one of the following conditions:

(a) for each characteristic p other than 2 of a field K in an "Oil and Vinegar" scheme of degree 2, v satisfies the inequality $q^{(v-n)-1} * n^4 > 2^{40}$, where K is a finite field over which the sets S1, S2 and S3 are provided,

(b) for p = 2 in an "Oil and Vinegar" scheme of degree 3, v is greater than n*(1 + sqrt(3)) and less than or equal to $n^3/6$, and

(c) for each p other than 2 in an "Oil and Vinegar" scheme of degree 3, v is greater than n and less than or equal to n^4.

Claim 42 (previously presented) Apparatus according to claim 40 and wherein the set S2 comprises a set S of k polynomial functions of a UOV scheme, and the number v of "vinegar" variables is selected to satisfy the inequalities $v<n^2$ and $q^{(v-n)-1} * n^4 > 2^{40}$ for a characteristic p=2 of a field K in an "Oil and Vinegar" scheme of degree 2, where K is a finite field over which the sets S1, S2 and S3 are provided and q is the number of elements of K.

Claim 43 (new) A method according to claim 1 and wherein the computing device comprises at least one of the following: a computer; and a smart card.

Claim 44 (new) Apparatus according to claim 18 and wherein the computer system comprises at least one of the following: a computer; and a smart card.